REPORT OF EXAMINATION | 2018M-235

City of Middletown

Information Technology

JANUARY 2020

OFFICE OF THE NEW YORK STATE COMPTROLLER
Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

City of Middletown

Audit Objective

Determine whether City officials ensured the City's Information Technology (IT) systems were adequately secured and protected against unauthorized use, access and loss.

Key Findings

- City officials did not develop adequate IT policies or procedures.
- 70 user accounts have not been used in the last six months, 19 of these accounts were never used and one account was last used to logon to the network more than nine years ago.
- Financial application users had excessive permissions.

In addition, sensitive IT control weaknesses were communicated confidentially to City officials.

Key Recommendations

- Adopt comprehensive written IT policies and procedures to address acceptable computer use and online banking.
- Develop written procedures for managing system access that include periodically reviewing user access.
- Limit financial application access to ensure City users cannot control all phases of a transaction.

City officials disagreed with certain aspects of our findings and recommendations, but indicated they have initiated or planned to initiate corrective action. Appendix B includes our comments on issues raised in the City's response letter.

Background

The City of Middletown is located in Orange County. The City is governed by a Mayor and a nine-member Common Council (Council). The Council is responsible for providing oversight of City operations. The Mayor is the chief executive officer and is responsible, along with other administrative staff, for the City's day-to-day administration.

City officials contract with a full-time IT specialist to provide IT support. The IT specialist is responsible for providing general IT support and managing the City-wide and police department networks.

Quick Facts	
IT User Accounts	240
2018 General Fund Appropriations	$39.8 million
IT Contract Expenditures for the Audit Period	$226,800

Audit Period

January 1, 2017 – July 19, 2018. We extended our audit period forward through October 22, 2018 to complete our IT testing.

Information Technology

How Should IT Systems Be Secured and Protected?

The City's IT system and data are valuable resources. The City relies on its IT system for internet access, email and for maintaining financial and personnel records. If the IT system is compromised, the results could be catastrophic and require extensive effort and resources to evaluate and repair. While effective controls will not guarantee the safety of a computer system, a lack of effective controls significantly increases the risk that data, hardware and software systems may be lost or damaged by inappropriate access and use.

A city's governing body should establish computer policies that take into account people, processes and technology; communicate these policies throughout the city's departments; and ensure city officials develop procedures to monitor compliance with the policies. New York State Technology Law[1] requires cities to have a breach notification policy or local law that requires certain individuals to be notified when there is a system security breach involving private information.

A computer use policy should be adopted that describes appropriate and inappropriate use of IT resources and compliance with that policy should be monitored by IT officials. Officials should also develop comprehensive written procedures for managing system access that include periodic reviews of user access to ensure that user accounts are disabled or deleted when access is no longer needed.

A disaster recovery plan provides a framework for reconstructing vital operations to resume time-sensitive operations and services after a disaster. Disasters may include any sudden, catastrophic event[2] that compromises the availability or integrity of an IT system and data.

Typically, a disaster recovery plan includes an analysis of business processes and continuity needs, disaster prevention instructions, specific roles of key individuals and precautions needed to maintain or quickly resume operations. Additionally, such a plan should include data backup procedures, such as ensuring a backup is stored off-site in case the building is destroyed or inaccessible, and periodic backup testing to ensure backups will function as expected.

Computer users must be aware of security risks and trained in practices that reduce internal and external threats to IT systems and data. While IT policies tell computer users what to do, IT security awareness training helps them understand their roles and responsibilities and provides them with the skills to perform them. Such training should center on:

1 New York State Technology Law, Section 208

2 Such as a fire, computer virus or inadvertent employee action

- Emerging trends in information theft and other social engineering reminders.
- Malicious software, virus protection and the dangers of downloading files and programs from the Internet.
- Password controls.
- Limiting the type of PPSI collected, accessed or displayed to that which is essential for the function being performed.
- Restricting physical access to IT systems and resources.
- Protecting IT systems from intentional or unintentional harm, loss or compromise.

Officials Did Not Develop Adequate Policies or Procedures

Although the City's employee manual requires City-owned computers and email accounts to be used for appropriate business purposes only, officials did not develop adequate written City-wide IT policies or procedures for acceptable computer use. We reviewed the technology use section of the employee manual and found that it did not clearly define use that was not acceptable or the consequences of violating the policy.

We reviewed the website browsing histories for 15 of the 85 computers with PPSI[3] and identified employees[4] who accessed websites not related to City-business. Employees accessed websites related to social media, entertainment and leisure. We also conducted an analysis of the shared folders on the network and found questionable use of City computer resources. For example, we identified folders that included music and electronic books related to gaming. Inappropriate or questionable use of computers could potentially expose the City to virus attacks that compromise systems and data, including key financial and confidential information.

When policies are not clearly communicated or defined, enforcement may be difficult. The IT specialist was unable to enforce the City's acceptable technology use policy because he was unaware such a policy existed. Furthermore, enforcing the policy would be difficult because the policy does not clearly define acceptable and non-acceptable use.

In our previous audit report,[5] we recommended that Council and City officials develop and adopt IT policies and procedures that include the breach notification requirement. The City's corrective action plan indicated that a breach notification

3 Refer to Appendix C for information on our sampling methodology.

4 We identified approximately 42 different user profiles on the 15 computers scanned.

5 Refer to our prior audit report, City of Middletown – Selected Financial Operations and Information Technology (2013M-56), issued in 2013.

policy would be developed during 2014. However, the Council did not adopt a breach notification policy until 2015, and City officials were unaware that the Council adopted this policy.

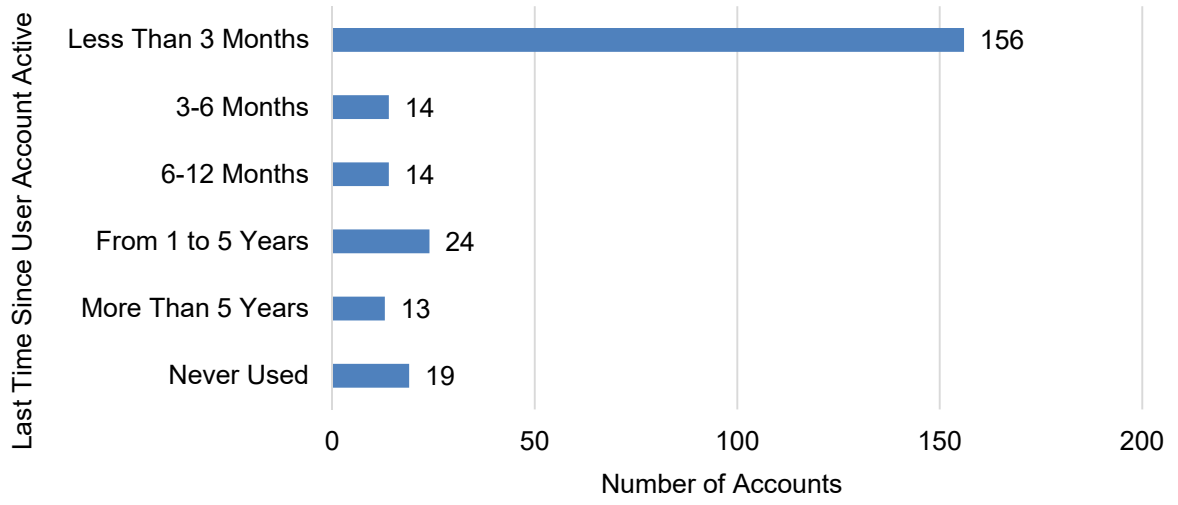
When officials and employees are unaware of a breach notification policy, they may not understand or fulfill their legal obligation to notify affected parties if private information is compromised, putting them at risk of losing financial or personal data.

Officials Did Not Develop Procedures for Managing System Access

City officials have not developed comprehensive written procedures for managing system access for the City's 240 user accounts. We found that 70 accounts were not used in the last six months. These 70 accounts are comprised of 35 generic user accounts, 31 user accounts for employees who do not regularly access the network, and four individuals no longer employed by the City. In addition, 19 of the 70 accounts were never used, and one account was last used to logon in March 2009, more than nine years ago.

FIGURE 1

User Account Login Activity



Having inactive user accounts that are not monitored increases the risk that these accounts could potentially be used by those individuals or others for malicious purposes.

Officials Have Not Developed a Disaster Recovery Plan

City officials have not developed a disaster recovery plan to address potential disasters. Consequently, in the event of a disaster, City officials have no guidelines to minimize or prevent the loss of equipment and data or to appropriately recover data. In our previous audit,[6] we recommended that Council and City officials develop and adopt a formal written disaster recovery plan to protect the City in the event of a disaster. City Officials did not take corrective action to address this important safeguard.

City officials did not provide a reason for not adopting a disaster recovery plan. Officials told us that they would contact the IT specialist, who would use backups to restore necessary programs, in the event of a disaster.

However, without a formal plan, the City could lose important equipment, financial and other data and suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees.

Officials Did Not Provide IT Security Awareness Training

City officials did not provide users with IT security awareness training to help ensure they understand IT security measures. As a result, there is an increased risk that users may not understand their responsibilities, putting the data and computer resources at greater risk for unauthorized access, misuse or abuse.

What Are Effective Financial Application Controls?

Officials should segregate duties within the financial application to ensure that employees are granted access needed to perform their duties but cannot perform all phases of a transaction. Additionally, audit logs should be reviewed to ensure individuals are making only authorized changes in the application. Any unusual or unauthorized activity could indicate a breakdown in controls or possible malfeasance.

City Users Had Excessive Access to the Financial Application

We found that four finance department employees[7] have administrative rights to the City's financial application. These users have the capability to access all functions within the software. Therefore, these users could add new users to the system, change users' access rights, and potentially perform all phases of a transaction. Of the four users, only the Treasurer and Deputy Treasurer need this

6 Ibid.

7 Treasurer, Deputy Treasurer, accounts payable clerk, and senior clerk.

level of access. The other two users should only have access needed to perform their job duties.

The Deputy Treasurer told us that the Treasurer, Deputy Treasurer and two additional employees were given administrative user access rights to ensure the department had an employee available at all times with override capabilities. However, this is not a valid justification for granting administrative access rights. In addition, officials do not review an audit log to ensure individuals are making only authorized changes and to compensate for the inadequate access controls. As a result, there is an increased risk that intentional or unintentional changes could occur without detection.

What Are Effective Online Banking Controls?

Online banking provides a means of direct access to funds held in City bank accounts. Users can review current account balances and account information, including recent transactions, and transfer money between bank accounts and to external accounts. Because funds transferred electronically typically involve significant amounts of money, City officials must control the processing of its electronic transfers to help prevent unauthorized transfers from occurring. It is essential that officials provide authorization of transfers before they are initiated and establish procedures to ensure that staff are securely accessing banking websites to help reduce the risk of unauthorized transfers from both internal and external sources.

GML[8] allows cities to disburse or transfer funds in their custody by means of electronic transfers, provided that the governing board has entered into a written agreement. GML requires that this agreement prescribe the manner in which electronic transfers will be accomplished and identify the names and numbers of bank accounts from which such transfers may be made and the individuals authorized to request transfers.

GML also requires the city to implement a security procedure that includes verifying that a payment order is for the initiating city and detecting payment order errors in transmission or content. An employee should not be able to execute an electronic transfer without obtaining authorization from the custodial officer or a deputy.

Municipalities should also check with their banks about enabling alerts and other security measures that may be available such as blocking wire transfers to foreign countries, email notifications and requiring the verification of transactions over certain amounts, possibly through callbacks. In addition, a city's governing body should adopt a policy that outlines the online banking activities city officials will

8 GML, Article 2, Section 5-A

engage in, specifies which employees are authorized to process transactions and establishes a detailed approval process to verify the accuracy and legitimacy of transactions.

To the extent possible, authorized users should access bank accounts from one computer dedicated for online banking from a wired network to minimize exposure to malicious software, because other computers may not have the same security protections as a dedicated computer.

Officials Lacked Adequate Banking Agreements

City officials maintain 21 bank accounts with three different banks for online banking transactions, which included electronic deposits, interaccount transfers and electronic withdrawals. We reviewed the banking agreements for all of these banks.

We found that one agreement was a standard procedure document that was not signed by either City officials or the bank. The two other agreements did not identify the bank account names and account numbers that transfers may be made from and one agreement did not identify the employees authorized to request transfers. In addition, officials did not establish security controls such as blocking transfers to foreign countries for two banks.

Without adequate online banking agreements or security controls, City officials cannot be assured that funds are adequately safeguarded when performing online bank transactions.

Officials Did Not Adequately Safeguard Online Banking Transactions

The Council did not adopt an online banking policy to establish which employees are authorized to process transactions or establish a detailed approval process to verify the accuracy and legitimacy of transactions before they are processed. In addition, a dedicated separate computer was not used for online banking activities and users were able to access online banking from non-City devices.

We reviewed user online banking access. Although all online banking procedures require one employee to initiate and another employee to approve a transaction, we found that one employee, who was able to initiate transactions, should not have been allowed to do so. The Deputy Treasurer told us that this employee should have been allowed only to read or view, but not initiate, online banking transactions.

All online banking users are required to enter a user name and password and a unique passcode that is generated each time they login.[9] However, the City does

9 A different unique passcode is generated when a user logs in.

not have a formal policy to safeguard cash during online banking transactions, prevent online banking from multiple devices or limit banking permissions. As a result, officials cannot ensure that employees are aware of their responsibilities and there is an increased risk of unauthorized access, exposure to malicious software, inappropriate activity and misappropriation of cash.

What Do We Recommend?

The Council should:

1. Adopt comprehensive IT policies that address acceptable use and online banking and communicate all adopted IT policies to City officials, employees and the IT specialist.[10]

2. Review and update IT policies at least once each year to keep them in line with changing technology.

City officials should:

3. Adopt written procedures for managing system access that include periodically reviewing user access and disabling or deleting user accounts when access is no longer needed.

4. Develop a comprehensive disaster recovery plan, and update and test the plan periodically.

5. Ensure that IT security awareness training is provided periodically to all employees who use computers.

6. Periodically review financial application access and limit access rights to ensure that user access to the financial application is properly segregated so that authorizing, transmitting, recording and approving transactions are segregated and that access is based on job function.

7. Periodically review audit logs to make sure employees are making only authorized entries in the financial accounting system.

8. Ensure that the City has a sufficient written online banking agreement with each bank in accordance with GML and that those who perform online banking transactions are familiar with its content.

9. Dedicate a separate computer for online banking activities and limit all online banking to that computer.

10. Periodically review online banking users and access rights and limit excessive online banking access.

10 Refer to our publication Information Technology Governance available at www.osc.state.ny.us/localgov/pubs/lgmg/itgovernance.pdf

Appendix A: Response From City Officials

Department of Finance

City of Middletown

16 James Street
Middletown, NY 10940-1587
Tel: (845) 346-4150
Fax: (845) 343-1101

December 11, 2019

[redacted]
Office of the State Comptroller
Division of Local Government and School Accountability
33 Airport Drive, Suite 103
New Windsor, New York 12553

Dear [redacted]

Below is Middletown's response to the information technology report of Examination # 2018M-235.

Prior to the responses I am requesting that you tone down the "headlines". For example, **"Officials Lacked Adequate Banking Agreements"** when in fact a couple of files were lacking a few documents. I discussed this with [redacted]he offered to review it. In other words please consider our responses prior to the issuance of the final report if you can.

See Note 1 Page 12

IT Related

Officials Did Not Develop Adequate Policies or Procedures

Response
The City will update the Policy.

Officials Did Not Develop Procedures for Managing System Access
City officials have not developed comprehensive written procedures for managing system access for the City's 240 user accounts. We found that 70 accounts were not used in the last six months. In addition, 19 of the 70 accounts were never used, and one account was last used to logon in March 2009, more than nine years ago.

Response
The City does not agree with the numbers reported. Of the 70 accounts identified there were 42 user accounts. Of the 42 user accounts, some of the user accounts do not directly log into the domain regularly. The remaining 28 accounts are system service accounts. When comparing user accounts to the current employee list, 6 user accounts were identified that needed to be removed.

See Note 2 Page 12

Corrective Action
The City will institute a formal procedure with HR to inform IT of employee terminations. The City will increase the frequency of comparing user accounts to the current employee list.

Officials Have Not Developed A Disaster Recovery Plan

Response
The City takes backup and security as a top priority in order to restore services in the event of a cyber-attack or loss of facilities. All systems are backed up regularly and are stored offsite.

Corrective Action
The City is in the process of developing a Formal Disaster Recovery Plan.

Officials Did Not Provide IT Security Awareness Training

Corrective Action
The City is evaluating proposals for IT Security Awareness Training for its employees.

Finance Related

City Users Had Excessive Access to the Financial Application

See Note 3 Page 12

Response
The City does not agree that there are too many finance employees with full access to financial and accounting systems.

The two employees other than the Treasurer and Deputy Treasurer process volumes of data to keep the City's general ledger and books of original entry current. Stopping work flow to obtain authority to finish the task at hand will greatly reduce efficiency.

Corrective Action
The Treasurer or Deputy will review transaction logs (Journal Entries) monthly.

Online Banking Control was Inadequate

Response
The City has a policy and standard practice that requires two bonded employees to wire funds. One to initiate and the second is to approve. This is done electronically and the bank also confirms that the computer being used is tied to the employee.

See Note 4 Page 12

Generally wire transfers are limited to critical issues such as payroll and related taxes and to pay certain large vendors. With mostly senior employees getting 4 to 5 weeks' vacation per year plus 15 holidays and many other paid absences annually the City needs this configuration of employees to process City business on a timely basis.

Corrective Action
The City will discuss options provided by [redacted] to provide an alert for transactions that seem questionable. Establish a list of vendors that the City uses wires to pay and put a bank stop in place for vendors not on the list.

Officials Lacked Adequate Banking Agreements

See Note 5 Page 12

A couple of files were incomplete. The City doesn't see this as a major problem.

Corrective Action
The City will review all files and conform them to the appropriate GML.

Officials Did Not Adequately Safeguard Online Banking Transaction

The City does not agree that officials did not adequately Safeguard Online Banking Transaction and does not believe having a single dedicated computer for this activity will provide better safeguards.

See Note 6 Page 13

This is further supported by decades of certified audits with no irregularities noted.

Corrective Action
Officials will develop an online banking policy and request Common Council approval.

Cordially,

Donald J. Paris
Treasurer

George Weissner
IT Manager

CC. Joseph DeStefano, Mayor
Janet Gallo, Deputy Treasurer

Appendix B: OSC Comments on the City's Response

Note 1

The headlines are a summation of the facts in the different sections of the report. City officials did not express any disagreement with the factual content of the report during the exit conference or throughout the audit process.

Note 2

We have amended our audit report to give context to the information on the 70 user accounts not used in the last six months. While six user accounts were identified as no longer employees, two of these accounts were mentioned in our confidential IT letter and not part of the 70 accounts mentioned in the audit report. These numbers are also based on the City's network settings as of October 22, 2018 and may differ from the City's current list of users.

Note 3

As stated in our report, officials should segregate duties within the financial application to ensure that employees are granted access needed to perform their duties but cannot perform all phases of a transaction. City officials did not adequately segregate duties within financial application or implement compensating controls. We found that four finance department employees had administrative permissions to the City's financial application, which allow them to add new users to the system, change users' access permissions, and potentially perform all phases of a transaction. At a minimum, officials should implement controls to compensate for the inadequate access controls. For example, officials could review audit logs to ensure individuals are making only authorized changes.

Note 4

Our audit report states that the Council did not adopt an online banking policy to establish which employees are authorized to process transactions or establish a detailed approval process to verify the accuracy and legitimacy of transactions before they are processed. Although all online banking procedures require one employee to initiate and another employee to approve a transaction, we found that one employee, who was able to initiate transactions, should not have been allowed to do so. Furthermore, officials did not establish security controls such as blocking transfers to foreign countries for two banks.

Note 5

As stated in our report, one agreement was a standard procedure document that was not signed by either City officials or the bank. The two other agreements did not identify the bank account names and account numbers that transfers may be made from and one agreement did not identify the employees authorized to request transfers. We agree with the City's corrective action to review all files and conform them to GML.

Note 6

There is no single control that is most effective for protecting information technology systems, information and local government resources. However, best practice advises this can be accomplished by building successive layers of defense mechanisms, a strategy referred to as defense-in-depth. This includes using a dedicated computer for online banking transactions, one that is not used for email or internet browsing. If City officials are unable to dedicate a computer for online banking, they should implement compensating controls to reduce online banking risks. For example, City officials could provide information security awareness training to educate users on safe computing practices such as being suspicious of emails purporting to be from their bank, avoid visiting un-trusted websites or opening suspicious emails.

Appendix C: Audit Methodology and Standards

We conducted this audit pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the New York State General Municipal Law. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- We reviewed the City's policy and procedure manuals to identify IT-related policies and evaluated those policies to gain an understanding of internal controls over IT.
- We interviewed officials and personnel to gain an understanding of internal controls over IT and online banking.
- We judgmentally selected a sample of 15 computers from the 85 users who had access to PPSI.[11] We reviewed web history reports for accessed websites that could put the network at risk. We selected those computers assigned to the Deputy Treasurer, senior account clerk and payroll clerk because their duties and privileges involved using and transmitting important electronic financial data. We selected the 12 other users based on their access to business applications and PPSI.
- We ran a shared folders audit script on both the City and police department domain controllers. We analyzed the report to identify any folders that could potentially contain files that indicated misuse of City computers. We then determined who had access to those folders and verified the contents of the folders with City officials.
- We ran an Active Directory[12] audit script on the City and police department domain controllers. We then analyzed the report for inactive users.
- We inquired about a disaster recovery plan.
- We reviewed user access rights for the City's financial application and evaluated permissions to determine whether user access is properly segregated and based on the need of the job function.
- We inquired about any written agreement with the City's banks and reviewed the agreements provided to determine whether they were in accordance with GML. We also inquired about any online banking policy.
- We reviewed user access rights for the online banking application and evaluated permissions to determine whether there was a proper segregation of access rights and if granted access rights were necessary for the employees to perform their assigned duties.

11 These users had access to key financial applications and related PPSI including online banking, payroll, and human resources.

12 Active Directory is a server database consisting of objects such as user and computer accounts along with their respective attributes (e.g., username display name). It provides a single point of network authentication and resource management.

Our audit also examined the adequacy of certain information technology controls. Because of the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to City officials.

We conducted this performance audit in accordance with GAGAS (generally accepted government auditing standards). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or relevant population size and the sample selected for examination.

The Council has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report should be prepared and provided to our office within 90 days, pursuant to Section 35 of General Municipal Law. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. We encourage the Council to make the CAP available for public review in the City Clerk's office.

Appendix D: Resources and Services

Regional Office Directory
www.osc.state.ny.us/localgov/regional_directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/localgov/costsavings/index.htm

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/localgov/fiscalmonitoring/index.htm

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/localgov/pubs/listacctg.htm#lgmg

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/localgov/planbudget/index.htm

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/localgov/pubs/cyber-security-guide.pdf

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller
www.osc.state.ny.us/localgov/finreporting/index.htm

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/localgov/researchpubs/index.htm

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.state.ny.us/localgov/academy/index.htm

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor, Albany, New York 12236

Tel: (518) 474-4037 • Fax: (518) 486-6479 • Email: localgov@osc.ny.gov

www.osc.state.ny.us/localgov/index.htm

Local Government and School Accountability Help Line: (866) 321-8503

NEWBURGH REGIONAL OFFICE – Lisa A. Reynolds, Chief Examiner

33 Airport Center Drive, Suite 103 • New Windsor, New York 12553-4725

Tel (845) 567-0858 • Fax (845) 567-0080 • Email: Muni-Newburgh@osc.ny.gov

Serving: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester counties

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller